IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 11bi D2.0 CRs in 10.71.8 | | | | |
| Date: 2025-09-11 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Jerome Henry | Cisco Systems |  |  | jerhenry@cisco.com |
| Domenico Ficara | Cisco Systems |  |  | dficara@cisco.com |
| Ugo Campiglio | Cisco Systems |  |  | ucampigl@cisco.com |
| Federico Lovison | Cisco Systems |  |  | flovison@cisco.com |

Abstract

This submission proposes resolutions for the following CIDs:

2288, 2438, 2273, 2439, 2440, 2441, 2255, 2442, 2283, 2443, 2444, 2284, 2457, 2458, 2459, 2460, 2461, 2462.

Revisions:

* Rev 0: Initial version of the document.

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbi D2.0 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbi D2.0 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents). TGbi Editor: Editing instructions preceded by “TGbi Editor” are instructions to the TGbi editor to modify existing material in the TGbi draft. As a result of adopting the changes, the TGbi editor will execute the instructions rather than copy them to the TGbi Draft.***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 2288 | 10.71.8 | 116.60 | "BSS privacy enhancements operations" belongs to clause 12 | Move the subclause into clause 11 | Rejected.  It is unclear what the recommendation is (clause 11 or 12). The BSS operations belong to the MAC layer, so clause 10 seems a relevant clause. Clause 11 is MLME, seems irrelevant, clause 12 is security, but BPE is about privacy, not specifically about security. |
| 2438 | 10.71.8 | 116.63 | Regarding the text "The BPE AP MLD privacy is protected by not sending BPE AP MLD discovery information, e.g., SSID, capability or operation elements, over the air in the clear.": This explanation is unusual because it says "[X] is protected by not [doing Y]". An active statement would be better | Replace the identified text with: "The BPE AP MLD privacy is protected by encrypting BPE AP MLD discovery information, e.g., SSID, capability or operation elements". | Revised  It is not that these elements are just encrypted, they are also not sent. TGbi editor to make the changes shown in the latest version of 11-25/1631 under all headings that include CID 2438. |
| 2273 | 10.71.8 | 117.10 | What is "BGTK"? Only one occurrence in this draft. Is it typo for PGTK? | Remove it or correct it. | Revised, typo indeed.  TGbi editor to make the changes shown in the latest version of 11-25/1631 under all headings that include CID 2273. |
| 2439 | 10.71.8 | 117.12 | "BPE MLD" should be "BPE AP MLD" | Replace "BPE MLD" with "BPE AP MLD" | Accepted  Note: TGbi editor to make the changes shown in the latest version of 11-25/1631 under all headings that include CID 2439 |
| 2440 | 10.71.8 | 117.15 | "BPE MLD" should be "BPE AP MLD" | Replace "BPE MLD" with "BPE AP MLD" | Accepted  Note: TGbi editor to make the changes shown in the latest version of 11-25/1631 under all headings that include CID 2440 |
| 2441 | 10.71.8 | 117.17 | Regarding the text "Integrity protected group addressed management frames can be received by eavesdroppers," All frames can be received, the important thing is that the payload data is not encrypted and so the payload data is available to eavesdroppers. | Replace the identified text with: "The (unencrypted) payload data of itegrity protected group addressed management frames is available to eavesdroppers," | Revised. TGbi editor to make the changes shown in the latest version of 11-25/1631 under all headings that include CID 2441. |
| 2255 | 10.71.8 | 117.20 | By "a single EPP group", does it mean if BPE is enabled, there will be only one EPP group? Non-AP MLDs cannot create other EPP groups when BPE enabled? Same issue in P117L21. | Suggest make the default group as BPE EPP group, BPE parameters are generated using this group, CPE parameters are generated using per-non-AP MLD EPP group. | Revised. TGbi editor to make the changes shown in the latest version of 11-25/1631 under all headings that include CID 2255. |
| 2442 | 10.71.8 | 117.20 | "non-AP BPE MLDs" should be "BPE Non-AP MLDs" | Replace "non-AP BPE MLDs" with "BPE Non-AP MLDs" | Revised. TGbi editor to make the changes shown in the latest version of 11-25/1631 under all headings that include CID 2442. |
| 2283 | 10.71.8 | 117.23 | "CPE anonymization" occurs only once, "CPE FA" occurs 17 times. | Change to "CPE FA" | Revised  In fact, it should be CPE MHA, as per CID 2443. TGbi editor to make the changes shown in the latest version of 11-25/1631 under all headings that include CID 2283. |
| 2443 | 10.71.8 | 117.23 | Regarding the text "CPE anonymization, see 10.71.3 (Establishing CPE MAC header anonymization parameter sets).": (a) "CPE anonymization" should be "CPE MHA" (b) The referenced clause only defines how the parameters are established, so should be introduced approrpiately. | Replace the identified text with: "CPE MHA using [arametrs established accord to 10.71.3 (Establishing CPE MAC header anonymization parameter sets)." | Revised. TGbi editor to make the changes shown in the latest version of 11-25/1631 under all headings that include CID 2443. |
| 2444 | 10.71.8 | 117.24 | Regarding the text "BPE anonymization, see 10.71.4 (Establishing BPE MAC header anonymization parameter sets)": (a) "BPE anonymization" should be "BPE MHA" (b) The referenced clause only defines how the parameters are established, so should be introduced approrpiately. | Replace the identified text with: "BPE MHA using [arametrs established accord to 10.71.4 (Establishing BPE MAC header anonymization parameter sets)." | Revised. TGbi editor to make the changes shown in the latest version of 11-25/1631 under all headings that include CID 2444. |
| 2284 | 10.71.8 | 117.25 | "BPE anonymization" occurs only once, "BPE FA" occurs 33 times. | Change to "BPE FA" | Revised  It should in fact be BPE MHA, as in CID 2444. TGbi editor to make the changes shown in the latest version of 11-25/1631 under all headings that include CID 2284. |
| 2457 | 10.71.8.3 | 119.07 | "A BPE AP" should be "A BPE AP MLD" | Replace "A BPE AP" with "A BPE AP MLD" | Accepted  Note: TGbi editor to make the changes shown in the latest version of 11-25/1631 under all headings that include CID 2457 |
| 2458 | 10.71.8.3 | 119.12 | "The receiver address" should be "The receiver address and transmitter address" | Replace "The receiver address" with "The receiver address and transmitter address" | Accepted  Note: TGbi editor to make the changes shown in the latest version of 11-25/1631 under all headings that include CID 2458 |
| 2459 | 10.71.8.3 | 119.21 | "A BPE affiliated STA" should be "A BPE non-AP MLD" | Replace "A BPE non-AP" with "A BPE non-AP MLD" | Accepted  Note: TGbi editor to make the changes shown in the latest version of 11-25/1631 under all headings that include CID 2459 |
| 2460 | 10.71.8.3 | 119.24 | "10.71.5.4 (Addressing)" should be "10.71.6.1.3 (Address filtering for BPE MHA)" | Replace "10.71.5.4 (Addressing)" with "10.71.6.1.3 (Address filtering for BPE MHA)" | Accepted  Note: TGbi editor to make the changes shown in the latest version of 11-25/1631 under all headings that include CID 2460 |
| 2461 | 10.71.8.3 | 119.25 | Regarding the text "-- The transmitter address is filtered as descried in 10.71.6.1 (Address filtering). -- The receiver address is deanonymized as described in 10.71.5.4 (Addressing).": The filtering based on both transmitter address and receiver address in teh BPE case is described in 10.71.6.1.3 (Address filtering for BPE MHA) | Replace the identified text with: "-- The transmitter address and receiver address are filtered as descried in 110.71.6.1.3 (Address filtering for BPE MHA)." | Accepted  Note: TGbi editor to make the changes shown in the latest version of 11-25/1631 under all headings that include CID 2461 |
| 2462 | 10.71.8.3 | 119.34 | "The BPE AP" should be "The BPE AP MLD" | Replace "The BPE AP" with "The BPE AP MLD" | Accepted  Note: TGbi editor to make the changes shown in the latest version of 11-25/1631 under all headings that include CID 2462 |

**Discussion**

Clauses before addressing CIDs

**10.71.8 BSS privacy enhancements operations**

BSS Privacy Enhancement (BPE) operations protect the privacy of BPE AP MLDs and associated BPE non-AP MLDs. The BPE AP MLD privacy is protected by not sending BPE AP MLD discovery information, e.g., SSID, capability or operation elements, over the air in the clear.

APs affiliated with a BPE AP MLD transmit Privacy Beacon frames 9.3.4.4 (Privacy Beacon frame format) instead of Beacon frames 9.3.3.2 (Beacon frame format). A BPE AP MLD is discoverable only by non-AP MLDs that have the preshared identity key of the BPE AP MLD as described in 10.71.8.1 (BPE AP MLD discovery).

A BPE AP MLD does not use beacon protection with a BIGTK or BIP with IGTK. A BPE non-AP MLD obtains from the protected (re)association response frame a GTK for each affiliated AP that it has a link, a BGTK and an Identity Key.

NOTE 1—An AP affiliated with a BPE MLD does not have BIGTK, because they do not transmit Beacon frames. Instead, they transmit Privacy Beacon frames, see (10.71.8.2(BPE AP MLD Beaconing).

NOTE 2—An AP affiliated with a BPE MLD does not have IGTK, because all group addressed management frames are encrypted by using the group cipher suite indicated for the BSS. IGTK integrity protects group addressed management frames. Integrity protected group addressed management frames can be received by eavesdroppers, which would reduce privacy of the BPE AP MLD.

The associated non-AP BPE MLDs and BPE AP MLD operate in a single EPP group. At the beginning of each epoch, the BPE non-AP STA addresses and SN spaces and PNs of the individual frames are anonymized in all links according to CPE anonymization, see 10.71.3 (Establishing CPE MAC header anonymization parameter sets). The BPE MLD affiliated AP addresses, the Timestamp field of the Privacy Beacons and the group frames are anonymized according to BPE anonymization, see 10.71.4 (Establishing BPE MAC header anonymization parameter sets). The AIDs used by the associated non-AP BPE MLDs are assigned by the AP MLD, see 10.71.7 (Frame anonymization and AID).

**10.71.8.3 Group addressed frames anonymization**

A BPE AP shall anonymize group addressed frames by using offsets as described in 10.71.4 (Establishing BPE MAC header anonymization parameter sets):

The MAC header anonymization parameters are selected as described in 10.71.5.1 (MAC header anonymization parameter set selection).

The receiver address is anonymized as described in 10.71.5.4 (Addressing).

The SN is anonymized with the SNS1 DL offset as described in 10.71.5.2 (Sequence number anonymization).

The PN is anonymized with the PN group offset as described in 10.71.5.3 (Packet number anonymization).

A BPE affiliated STA shall deanonymize the received group frames by using the offsets as described in 10.71.4 (Establishing BPE MAC header anonymization parameter sets):

The transmitter address is filtered as descried in 10.71.6.1 (Address filtering).

The receiver address is deanonymized as described in 10.71.5.4 (Addressing).

The PN is deanonymized with the PN group offset as described in 10.71.6.3 (Packet number deanonymization).

The SN is deanonymized with the SNS1 DL offset as described in 10.71.6.4 (Sequence number deanonymization).

The BPE AP shall use GTK to encrypt the payload of the group addressed Management frames.

CID 2438

Accepted

BSS Privacy Enhancement (BPE) operations protect the privacy of BPE AP MLDs and associated BPE non-AP MLDs. The BPE AP MLD privacy is ~~protected~~ achieved (#2438) by removing the need to send (#2438) ~~not sending~~ BPE AP MLD discovery information, e.g., SSID, capability or operation elements, over the air in the clear.

CID 2273

Revised

A BPE AP MLD does not use beacon protection with a BIGTK or BIP with IGTK. A BPE non-AP MLD obtains from the protected (re)association response frame a GTK for each affiliated AP that it has a link, a P~~B~~GTK (#2273) and an Identity Key.

CID 2439, 2440

Accepted

NOTE 1—An AP affiliated with a BPE AP (#2439) MLD does not have BIGTK, because they do not transmit Beacon frames. Instead, they transmit Privacy Beacon frames, see (10.71.8.2(BPE AP MLD Beaconing).

NOTE 2—An AP affiliated with a BPE AP (#2440) MLD does not have IGTK, because all group addressed management frames are encrypted by using the group cipher suite indicated for the BSS. IGTK integrity protects group addressed management frames. Integrity protected group addressed management frames can be received by eavesdroppers, which would reduce privacy of the BPE AP MLD.

CID 2441

Revised

NOTE 2—An AP affiliated with a BPE AP (#2440) MLD does not have IGTK, because all group addressed management frames are encrypted by using the group cipher suite indicated for the BSS. IGTK integrity protects group addressed management frames. Integrity protected group addressed management frames can be ~~received~~ intercepted and read (#2441) by eavesdroppers, which would reduce privacy of the BPE AP MLD.

CID 2255

~~The associated non-AP BPE MLDs and BPE AP MLD operate in a single EPP group.~~

The BPE AP defines a single EPP group, and all non-AP-MLDs associated to the BPE AP MLD are part of that single EPP group. A non-AP MLD cannot create or join another group, and a consequence of leaving the default EPP group is to stop CPE FA operations for the non-AP MLD.

When the associating non-AP MLD includes in the protected (re)association request an EPP element with the parameters of the EPP group it wishes to join, and when these parameters are incompatible with the parameters of the single group in operation on the BPE AP MLD (for example, and not limited to, the epoch duration is smaller than the value of the Min Epoch Pacing field included in the EPP Epoch Setting field of the EPP element, or the group ID value does not match the BPE AP EPP group ID), the BPE AP can either reject the association, ignore the EPP element and place the non-AP MLD in the BPE group, accept the association but not place the non-AP MLD in the BPE group (in which case the non-AP MLD does not have CPE FA operations activated), or change the values of the BPE group to make them compatible with the non-AP MLD requirements while still staying compatible with the requirements of some or all of the already associated other non-AP MLDs. (#2255)

At the beginning of each epoch, the BPE non-AP STA addresses and SN spaces and PNs of the individual frames are anonymized in all links according to CPE anonymization, see 10.71.3 (Establishing CPE MAC header anonymization parameter sets). The BPE MLD affiliated AP addresses, the Timestamp field of the Privacy Beacons and the group frames are anonymized according to BPE anonymization, see 10.71.4 (Establishing BPE MAC header anonymization parameter sets). The AIDs used by the associated non-AP BPE MLDs are assigned by the AP MLD, see 10.71.7 (Frame anonymization and AID).

CID 2283, 2443

Revised

At the beginning of each epoch, the BPE non-AP STA addresses and SN spaces and PNs of the individual frames are anonymized in all links ~~according to~~ by applying CPE MHA, using parameters described in (#2283, #2443) ~~anonymization, see~~ 10.71.3 (Establishing CPE MAC header anonymization parameter sets). The BPE MLD affiliated AP addresses, the Timestamp field of the Privacy Beacons and the group frames are anonymized according to BPE anonymization, see 10.71.4 (Establishing BPE MAC header anonymization parameter sets). The AIDs used by the associated non-AP BPE MLDs are assigned by the AP MLD, see 10.71.7 (Frame anonymization and AID).

CID 2284, 2444

Revised

At the beginning of each epoch, the BPE non-AP STA addresses and SN spaces and PNs of the individual frames are anonymized in all links by applying CPE MHA, using parameters described in (#2283, #2443) 10.71.3 (Establishing CPE MAC header anonymization parameter sets). The BPE MLD affiliated AP addresses, the Timestamp field of the Privacy Beacons and the group frames are anonymized ~~according~~ by applying ~~to~~ BPE MHA ~~anonymization~~ (#2284, #2444), using parameters described in ~~see~~ 10.71.4 (Establishing BPE MAC header anonymization parameter sets). The AIDs used by the associated non-AP BPE MLDs are assigned by the AP MLD, see 10.71.7 (Frame anonymization and AID).

CID 2457, 2459, 2462

Accepted

A BPE AP MLD(#2457) shall anonymize group addressed frames by using offsets as described in 10.71.4 (Establishing BPE MAC header anonymization parameter sets):

The MAC header anonymization parameters are selected as described in 10.71.5.1 (MAC header anonymization parameter set selection).

The receiver address is anonymized as described in 10.71.5.4 (Addressing).

The SN is anonymized with the SNS1 DL offset as described in 10.71.5.2 (Sequence number anonymization).

The PN is anonymized with the PN group offset as described in 10.71.5.3 (Packet number anonymization).

A BPE non-ALP MLD (#2459) affiliated STA shall deanonymize the received group frames by using the offsets as described in 10.71.4 (Establishing BPE MAC header anonymization parameter sets):

The transmitter address is filtered as descried in 10.71.6.1 (Address filtering).

The receiver address is deanonymized as described in 10.71.5.4 (Addressing).

The PN is deanonymized with the PN group offset as described in 10.71.6.3 (Packet number deanonymization).

The SN is deanonymized with the SNS1 DL offset as described in 10.71.6.4 (Sequence number deanonymization).

The BPE AP MLD (#2462) shall use GTK to encrypt the payload of the group addressed Management frames.

CID 2458

Accepted

A BPE AP MLD(#2457) shall anonymize group addressed frames by using offsets as described in 10.71.4 (Establishing BPE MAC header anonymization parameter sets):

The MAC header anonymization parameters are selected as described in 10.71.5.1 (MAC header anonymization parameter set selection).

The receiver address and transmitter address are (#2458) ~~is~~ anonymized as described in 10.71.5.4 (Addressing).

The SN is anonymized with the SNS1 DL offset as described in 10.71.5.2 (Sequence number anonymization).

The PN is anonymized with the PN group offset as described in 10.71.5.3 (Packet number anonymization).

CID 2460, 2461

Accepted

Discussion/note: 10.71.6.1.3 is called filtering, but it is also about address deanonymization, maybe the clause should be called both

A BPE non-ALP MLD (#2459) affiliated STA shall deanonymize the received group frames by using the offsets as described in 10.71.4 (Establishing BPE MAC header anonymization parameter sets):

The transmitter address is filtered as described in 10.71.6.1.3 (Address filtering for BPE MHA (#2461)).

The receiver address is deanonymized as described in 10.71.6.1.3 (Address filtering for BPE MHA) (#2460) ~~10.71.5.4 (Addressing)~~.

The PN is deanonymized with the PN group offset as described in 10.71.6.3 (Packet number deanonymization).

The SN is deanonymized with the SNS1 DL offset as described in 10.71.6.4 (Sequence number deanonymization).

*TGbi editor: Modify clauses 10.71.8 and 10.71.8.3 as follows (track change on – changes from version after 11-25/626):*

**10.71.8 BSS privacy enhancements operations**

BSS Privacy Enhancement (BPE) operations protect the privacy of BPE AP MLDs and associated BPE non-AP MLDs. The BPE AP MLD privacy is achieved (#2438) by removing the need to send BPE AP MLD discovery information, e.g., SSID, capability or operation elements, over the air in the clear.

APs affiliated with a BPE AP MLD transmit Privacy Beacon frames 9.3.4.4 (Privacy Beacon frame format) instead of Beacon frames 9.3.3.2 (Beacon frame format). A BPE AP MLD is discoverable only by non-AP MLDs that have the preshared identity key of the BPE AP MLD as described in 10.71.8.1 (BPE AP MLD discovery).

A BPE AP MLD does not use beacon protection with a BIGTK or BIP with IGTK. A BPE non-AP MLD obtains from the protected (re)association response frame a GTK for each affiliated AP that it has a link, a PGTK (#2273) and an Identity Key.

NOTE 1—An AP affiliated with a BPE AP (#2439) MLD does not have BIGTK, because they do not transmit Beacon frames. Instead, they transmit Privacy Beacon frames, see (10.71.8.2(BPE AP MLD Beaconing).

NOTE 2—An AP affiliated with a BPE AP (#2440) MLD does not have IGTK, because all group addressed management frames are encrypted by using the group cipher suite indicated for the BSS. IGTK integrity protects group addressed management frames. Integrity protected group addressed management frames can be intercepted and read (#2441) by eavesdroppers, which would reduce privacy of the BPE AP MLD.

The BPE AP defines a single EPP group, and all non-AP-MLDs associated to the BPE AP MLD are part of that single EPP group. A non-AP MLD cannot create or join another group, and a consequence of leaving the default EPP group is to stop CPE FA operations for the non-AP MLD.

When the associating non-AP MLD includes in the protected (re)association request an EPP element with the parameters of the EPP group it wishes to join, and when these parameters are incompatible with the parameters of the single group in operation on the BPE AP MLD (for example, and not limited to, the epoch duration is smaller than the value of the Min Epoch Pacing field included in the EPP Epoch Setting field of the EPP element, or the group ID value does not match the BPE AP EPP group ID), the BPE AP can either reject the association, ignore the EPP element and place the non-AP MLD in the BPE group, accept the association but not place the non-AP MLD in the BPE group (in which case the non-AP MLD does not have CPE FA operations activated), or change the values of the BPE group to make them compatible with the non-AP MLD requirements while still staying compatible with the requirements of some or all of the already associated other non-AP MLDs. (#2255)

At the beginning of each epoch, the BPE non-AP STA addresses and SN spaces and PNs of the individual frames are anonymized in all links by applying CPE MHA, using parameters described in (#2283, #2443) 10.71.3 (Establishing CPE MAC header anonymization parameter sets). The BPE MLD affiliated AP addresses, the Timestamp field of the Privacy Beacons and the group frames are anonymized by applying BPE anonyMHA, using parameters described in (#2284, #2444) 10.71.4 (Establishing BPE MAC header anonymization parameter sets). The AIDs used by the associated non-AP BPE MLDs are assigned by the AP MLD, see 10.71.7 (Frame anonymization and AID).

**10.71.8.3 Group addressed frames anonymization**

A BPE AP MLD (#2457) shall anonymize group addressed frames by using offsets as described in 10.71.4 (Establishing BPE MAC header anonymization parameter sets):

The MAC header anonymization parameters are selected as described in 10.71.5.1 (MAC header anonymization parameter set selection).

The receiver address and transmitter address are (#2458) anonymized as described in 10.71.5.4 (Addressing).

The SN is anonymized with the SNS1 DL offset as described in 10.71.5.2 (Sequence number anonymization).

The PN is anonymized with the PN group offset as described in 10.71.5.3 (Packet number anonymization).

A BPE non-AP MLD (#2459) affiliated STA shall deanonymize the received group frames by using the offsets as described in 10.71.4 (Establishing BPE MAC header anonymization parameter sets):

The transmitter address is filtered as described in 10.71.6.1.3 (Address filtering for BPE MHA (#2461)).

The receiver address is deanonymized as described in 10.71.6.1.3 (Address filtering for BPE MHA (#2460)).

The PN is deanonymized with the PN group offset as described in 10.71.6.3 (Packet number deanonymization).

The SN is deanonymized with the SNS1 DL offset as described in 10.71.6.4 (Sequence number deanonymization).

The BPE AP MLD (#2462) shall use GTK to encrypt the payload of the group addressed Management frames.